

REMARKS

This amendment is submitted in response to an Office Action mailed on June 4, 2007.

In the Office Action, all of pending claims 2-18 were rejected under 35 U.S.C. §103(a) as allegedly obvious over a base combination of art including U.S. Patent No. 6,999,587 to Asano et al. (the "Asano Patent") and U.S. Patent No. 7,065,216 to Benaloh et al. (the "Benaloh Patent"). Claims 15 and 16 were objected to because of informalities.

By the present paper, Applicants have amended claims 15 and 16 (as recommended by the Examiner), but Applicants respectfully traverse the rejection of claims based on the Asano and Benaloh Patents. Because each rejection of claims is predicated upon this base combination, and because this base combination does not support the position of the Examiner, the §103(a) rejection should be withdrawn as to all presented claims. Applicants additionally traverse the Examiner's combinations of base art with U.S. Patent No. 6,141,681 to Kyle (the "Kyle Patent") and U.S. Patent No. 6,529,950 to Lumelsky et al. (the "Lumelsky Patent"), for reasons presented in the discussion section, below. Because these combinations are improper, the rejection of claims 3-11, 13 and 16 (based on the Kyle Patent) and claim 14 (based on the Lumelsky Patent) also cannot stand.

Reconsideration of the outstanding rejection of claims is therefore respectfully requested.

I. Discussion.

A. The Present Invention.

The invention represented by the Applicants' claims at-issue relates to flexible watermarking capabilities that can be used to trace unauthorized copying back to a particular device. [See, e.g., paragraphs 56 and 174 of Applicants' specification.] Applicants' invention addresses the problem where many consumer electronics devices provide little or no real protection against copying, and the few content protection standards that are deployed in consumer electronics devices tend to be simple, rigid schemes that are difficult to upgrade and offer little real protection. [See, e.g.,

paragraphs 4 and 5 of Applicants' specification.] To this end, Applicants' propose devices and methods for improved security and for tracking sources of unauthorized content and taking mitigating action. In more specific forms of the invention, Applicants propose devices and methods that provide publishers with the ability to define their own security requirements, by allowing updateable policies that consider a wide variety of factors and determine whether (or how) to play in each environment. [See, e.g., paragraph 39 of Applicants' specification.] By providing these capabilities, the present invention facilitates renewability of security, because each newly mastered work or new release can implement different or more sophisticated security policies that better address evolving threats of unauthorized use or copying.

The claimed invention addresses these issues specifically in the context of broadcast encryption, that is, where content is distributed in a common broadcast format and is accessible to privileged users only, e.g., via encryption that only privileged users can decrypt. In the context of the invention of claim 2, broadcast encryption is decoded by players having cryptographic keys and protocols that must be used to decrypt the content. [See, e.g., claim 2, element (c).] The present invention facilitates a system that can make use of broadcast subscription cryptographic keys in the context of a common disk that is widely released. By employing multiple, alternate versions for each one of several regions within content, and by using unique combinations of player cryptographic keys (e.g., distributed as part of subscription to permit decryption), each player may be made to output only a single, unique version of content. The broadcast subscription scheme can thereby be adapted to uniquely watermark player output (even though all subscribers receive the same broadcast). [See, e.g., claim 2, element (d).] Further, by configuring distributed media to have a revocation list section for revoking other *media*, each new media distribution can facilitate remedial action to address detected misuse of prior media, e.g., a disk that was the subject of unauthorized use can be revoked, as can unauthorized copies of that disk. [See, e.g., claim 2, elements (a) and (b).]

More detailed features of Applicants' invention provide a renewable security system, that is, where security policies may be defined by a publisher to provide for security that may evolve to address previously successful security attacks. [See, e.g.,

paragraphs 93-94 and 187-188 of Applicants' specification.] To this end and, contrary to conventional wisdom, disk players may be made to execute code distributed with content to prevent playback unless a plurality of security checks are met. [See, e.g., Applicants' claim 3.] This code may be resident on a distributed disk and may be configured in a manner unique to each disk release, with security measures specified by each individual content publisher. That is to say, detailed features of the present invention provide a flexible system where the content itself can employ publisher-defined security processes that can vary from content-to-content to address new security needs, and not be made solely dependent on media player manufacturer designs.

B. The Invention Of Claims 2-18 Cannot be Considered As Obvious Over Combinations Involving The Asano And Benaloh Patents.

A rejection for obviousness is based on the underlying factual inquiries set forth in *Graham v. John Deere*: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims at issue; (3) the level of ordinary skill in the art; and (4) objective evidence of secondary considerations. Applicants here focus on the first two factors.

The apparent scope and content of the cited art is as follows. The Benaloh Patent relates to an in-flight entertainment system where it is desirable to have traceability to each in-flight player; to address this issue, the Benaloh Patent proposes content having uniquely marked portions, each portion copied to create a partition set, with each member of a given partition set being uniquely marked. The Benaloh Patent calls for distributing unique key set combinations to each in-flight player, such that each in-flight player can uniquely fingerprint its output. The Asano Patent relates to extending an illegal copy prevention scheme from read-only disks (such as DVDs) to user-recordable media; however, contrary to the Examiner's assertion, the Asano Patent has nothing whatsoever to do with broadcast encryption, at least not one of the type contemplated by Applicants. The Asano Patent provides a scheme where a user desiring to copy protect his or her personal, recorded media combines together both a content-specific key (k_m) and a unique pattern embedded into a non-writeable portion of

disk (i.e., magnetic fibers embedded during disk manufacturer near the center of the disk to create an inherent, unique fingerprint for each disk), to thereby generate a new content key. [See, e.g., column 6, lines 32-44 of the Asano Patent.] Utilizing this scheme, an end-user seeking to record video can deter theft since simply copying the content onto a new disk will fail to produce a useable key (because the correct key can only be recovered using the magnetic particle pattern on the original user-recorded disk. [See, e.g., column 14, lines 51-63, and column 16, lines 38-46 of the Asano Patent.] Simply put, the Asano Patent discloses a way to protect user-written media such that it can only be played on its original disk, but would not be usable with a broadcast encryption system (i.e., any recipient of an original disk made according to teachings of the Asano Patent may play that disk if that recipient has the media key, and there is no disclosure in, or apparent application of, the Asano Patent to use a large number of keys).

Assuming combination of the cited references by the Examiner is proper, what the combined art suggests is that writable disks may be made secure against copying using the scheme of the Asano Patent, and a small set of video players may be subjected to a scheme to fingerprint their output via the system of the Benaloh Patent.

The differences between the cited art and the claims at issue are substantial.

First, all of Applicants' claims requires a broadcast encryption scheme, that is, one where a common signal is distributed in a way such that only privileged users can read and interpret the content. The art relied upon by the examiner does not relate, show or suggest a broadcast encryption where multiple keys are used to fingerprint individual media, where further, an individual medium may be later revoked via this scheme. Furthermore, Claims 2-15 and 19-20 call for a list identifying at least one other medium that is revoked, also not shown by the cited art. The Asano Patent discloses a revocation table for revoking manufacturer certificates, but it does not show a revocation table for revoking a medium. [See, e.g., Column 8, lines 18-24 of the Asano Patent; "Here, the revocation list is such that the trusted center has made a digital signature on the version number thereof which increases monotonously and the *identification information ID of the manufacturer to which the secret key has been revealed and which is determined to have committed a fraud*" (emphasis added)]. By providing a

mechanism for publishing revocation of media, the present invention provides a feature whereby future content can revoke the specific medium that was the subject of improper use, copying or distribution (as detected using a fingerprinting scheme and tying fingerprint to specific media), as well as unauthorized copies stemming from that medium. There is nothing in the Asano or Benaloh Patents that teaches the desirability of or that presents a system of, revoking specific media.

Taking the obviousness inquiry as a whole, it is respectfully submitted that these differences are such that one of ordinary skill at the time of invention would not have considered the present invention as obvious. There is nothing in the cited art that suggests that one should, for example, use teachings of the Benaloh Patent to fingerprint the output of broadcast encryption video, and then provide for enforcement and revocation (for some reason not explained by the Examiner) by borrowing the writeable-disk invention of the Asano Patent but instead modifying it to (a) provide a revocations list of specific media, and (b) use the fingerprinting provided via the Benaloh technique together with a unique media identifier (i.e., thereby enabling tracking of specific media and revocation of specific media that was the subject of detected improper use or distribution). There is also nothing in the Asano or Benaloh Patents that teaches how one may later revoke unauthorized copies of content – if the Asano Patent were applied to such a scheme, its teachings would call for revoking blank discs made by a manufacturer identified via a revocations list, and would provide no mechanism for revoking a group of unauthorized copies that stem from a specific source.

It is respectfully submitted that the present invention cannot be considered unpatentable over combination of the Benaloh and Asano Patents. Even if their teachings are combined as advanced by the Examiner, the combination would still not operate to perform the same function as the claimed invention. Applicants submit that this fact is strong evidence of patentability, even in the post-KSR world, and that the rejection of claims based on the Benaloh and Asano Patents cannot be maintained.

C. The Invention Of Claims 3-11, 13 And 16 Cannot be Considered As Obvious Over Combinations Involving The Asano, Benaloh and Kyle Patents.

As mentioned earlier, it is one end of Applicants' invention to provide publishers with the ability to define their own security requirements, by allowing distributed programs or media to implement policies that consider a wide variety of factors and to determine whether (or how) to play in each environment. [See, e.g., paragraph 39 of Applicants' specification.] By providing these capabilities, the present invention facilitates renewability of security, because each newly-distributed work or broadcast can implement different or more sophisticated security policies that better address evolving threats of unauthorized copying. As a result, products can be brought to market more quickly by removing the need for player designers to anticipate and mitigate each possible attack.

More detailed features of the present invention facilitate this ability through the use of media-resident program logic and the presence of an interpreter in a player, to perform additional security checks that may be upgraded with each new distribution or broadcast. [See, e.g., claims 3-11, 13 and 16.] That is to say, code can be bundled with content, where the code is loaded onto and executed by a media player (not limited to general purpose computing platforms). Put perhaps another way, the invention of these claims creates a scheme where video disk players may be made to execute per-disk code (ideally written in a Turing complete language), to implement ad-hoc security functions that are not solely dependent on the original manufacturer's design of the player. For example, as indicated at paragraph 181 of Applicants' specification, in order to prevent adversaries from bypassing a media identity check, code may cause decryption processes to require multiple, non-standard checks of the originality of the playing media.

The Examiner predicates his position of unpatentability of these claims upon a combination of the Asano and Benaloh Patents, discussed above, and further, the Kyle Patent.

The Kyle Patent relates to communication between two computers with different operating systems for the purpose of transferring data; in particular, if the computers are incompatible, transferred data may be unintelligible by the receiving computer. To solve

this problem, the Kyle patent indicates that a translator file ("interpreter") should be downloaded so as to convert data from a first computer to a format understood by the second computer.

The Examiner cites the Kyle Patent to support his position that the bundled code /program logic feature of Applicants' invention is unpatentable.

Applicants respectfully disagree. As the explanation above should make clear, the translation file of the Kyle Patent has nothing to do with the security of media players. Applicants' invention relative to the claims at-issue relates to enabling content publishers to programmatically control a downstream device to provide enhanced security, and proposes to do so by bundling program logic directly with content, e.g., together on a video disk. One faced with a security problem of providing better security for media players, would not have at the time of invention "obviously" turned to a software translator to solve this problem.

What the Examiner has effectively done is to assume that Applicants invention is already part of the prior art and then to suggest, using this "straw man," that it would have been obvious, once media players were modified to use a software approach, to use an instruction set translator to deal with a possible problem of differing media player operating systems. Applicants respectfully submit that the Examiner's approach is improper, i.e., there are no teachings in the cited art that suggest that one should bundle code with program logic to promote enhanced content security and renewability. It is therefore requested that the Examiner withdraw any rejections that are predicated upon the Kyle Patent.

D. The Invention Of Claim 14 Cannot be Considered As Obvious Over Combinations Involving The Asano, Benaloh and Lumelsky Patents.

The Lumelsky Patent relates to a resource management framework that provides an object-oriented system for setup and control of a server-client media session. The Examiner incorrectly takes the position that the Lumelsky Patent "discloses means for reducing output quality of the audiovisual content if a security requirement..." is not met.

Applicants respectfully disagree. The Examiner's citations to the Lumelsky Patent indicate that "... the negotiator may have user quality preferences, cost

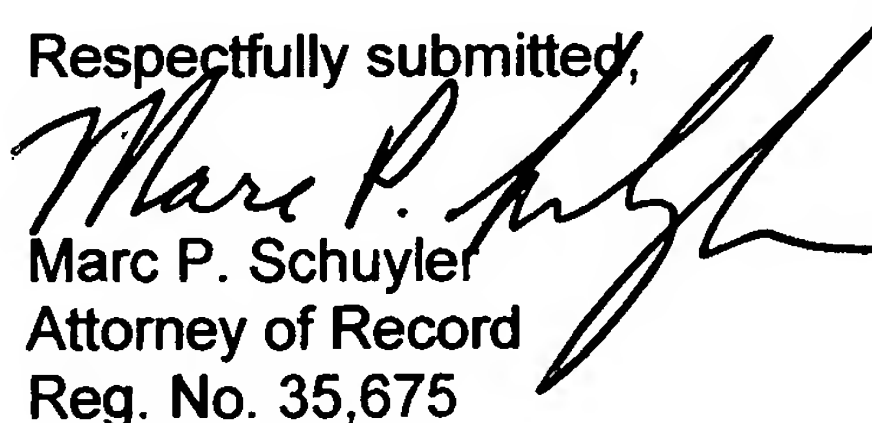
preferences, access authorizations, etc., that may modify the mapping set when applied.... For example, the user's preference may be for high quality content but may not wish to pay more than a certain amount which when exceeded a lower quality is acceptable if the costs target can be reached." The Examiner's citations do not reference any security requirement at all, nor do they suggest that one faced with media piracy deterrent goals should, using program logic that detects a possible insecure environment, reduce output quality. In fact, the cited portions of the Lumelsky Patent do not suggest that one should "change" or alter media quality at all, but rather, that *if* multiple alternate streams are available, including a high quality stream and a low quality stream, that a media server may use user preferences to select between them.

It is respectfully submitted that no art of record teaches or suggests reducing output quality at all, much less as a function of program logic identification of possible security issues, as a means of deterring piracy. Applicants submit that these differences between the cited art and the invention of claim 14 are such that an obviousness rejection cannot be maintained. It is therefore respectfully submitted that, in addition to the reasons advanced earlier, the rejection of claim 14 must be withdrawn, as this claim cannot be considered unpatentable over teachings of the Lumelsky Patent.

II. Conclusion.

It is respectfully submitted for the reasons indicated above that the present invention cannot be considered unpatentable over the art combinations cited by the Examiner. The differences between the cited art and the claims at-issue are significant. For the reasons advanced above, the Examiner is requested to reconsider the outstanding rejection.

Respectfully submitted,


Marc P. Schuyler
Attorney of Record
Reg. No. 35,675

Law Offices Of Marc P. Schuyler
P.O. Box 2535
Saratoga, CA 95070
(408) 655-6375